Federal Election Commission

Office of Inspector General

Final Report

Audit of the Federal Election Commission's Fiscal Year 2014 Financial Statements

November 2014

Assignment No. OIG-14-04

FEDERAL ELECTION COMMISSION
WASHINGTON, D.C. 20463
Office of Inspector General

MEMORANDUM

TO: The Commission

FROM: Inspector General

SUBJECT: Audit of the Federal Election Commission's Fiscal Year 2014 Financial Statements

DATE: November 17, 2014

Pursuant to the Chief Financial Officers Act of 1990, commonly referred to as the "CFO Act," as amended, this letter transmits the Independent Auditor's Report issued by Leon Snead & Company (LSC), P.C. for the fiscal year ending September 30, 2014. The audit was performed under a contract with, and monitored by, the Office of Inspector General (OIG), in accordance with auditing standards generally accepted in the United States of America; the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States; and applicable provisions of Office of Management and Budget (OMB) Bulletin No. 14-02, *Audit Requirements for Federal Financial Statements*.

Opinion on the Financial Statements

LSC audited the balance sheet of the Federal Election Commission (FEC) as of September 30, 2014 and the related statements of net cost, changes in net position, budgetary resources, and custodial activity (the financial statements) for the year then ended. The objective of the audit was to express an opinion on the fair presentation of those financial statements. In connection with the audit, LSC also considered the FEC's internal control over financial reporting and tested the FEC's compliance with certain provisions of applicable laws and regulations that could have a direct and material effect on its financial statements. The financial statements of the FEC as of September 30, 2013 were also audited by LSC whose report dated December 13, 2013, expressed an unmodified opinion on those statements.

In LSC's opinion, the financial statements present fairly, in all material respects, the financial position, net cost, changes in net position, budgetary resources, and custodial activity of the FEC as of, and for the year ending September 30, 2014, in conformity with accounting principles generally accepted in the United States of America.

Report on Internal Control

In planning and performing the audit of the financial statements of the FEC, LSC considered the FEC's internal control over financial reporting (internal control) as a basis for designing auditing procedures for the purpose of expressing their opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the FEC's internal control. Accordingly, LSC did not express an opinion on the effectiveness of the FEC's internal control.

Because of inherent limitations in internal controls, including the possibility of management override of controls; misstatements, losses, or noncompliance may nevertheless occur and not be detected. According to the American Institute of Certified Public Accountants:

- A **deficiency** in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis.
- A **significant deficiency** is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness yet important enough to merit attention by those charged with governance.
- A **material weakness** is a deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis.

LSC's consideration of internal control was for the limited purpose described in the first paragraph in this section and would not necessarily identify all deficiencies in internal control that might be significant deficiencies or material weaknesses. LSC did not identify any deficiencies in internal control that LSC would consider to be material weaknesses, as defined above. However, LSC did identify a significant deficiency in internal controls related to Information Technology security.

Report on Compliance with Laws and Regulations

FEC management is responsible for complying with laws and regulations applicable to the agency. To obtain reasonable assurance about whether FEC's financial statements are free of material misstatements, LSC performed tests of compliance with certain provisions of laws and regulations, noncompliance which could have a direct and material effect on the determination of financial statement amounts, and certain other laws and regulations specified in OMB Bulletin No. 14-02, *Audit Requirements for Federal Financial Statements*. LSC did not test compliance with all laws and regulations applicable to FEC.

The results of LSC's tests of compliance with laws and regulations described in the audit report disclosed one instance of noncompliance with The Homeland Security Presidential Directive 23, and National Security Presidential Directive 54, *Cyber Security and Monitoring*, establishing the Comprehensive National Cyber Security Initiative (the CNCI), and relating to Initiative No. 1, *Manage the Federal Enterprise Network as a Single*

Enterprise with a Trusted Internet Connection (TIC). Additional details can be found on page 13 of the audit report.

Audit Follow-up

The independent auditor's report contains recommendations to address deficiencies found by the auditors. Management was provided a draft copy of the audit report for comment and generally concurred with some of the findings and recommendations. In accordance with OMB Circular No. A-50, *Audit Follow-up*, revised, the FEC is to prepare a corrective action plan that will set forth the specific action planned to implement the agreed upon recommendations and the schedule for implementation. The Commission has designated the Chief Financial Officer to be the audit follow-up official for the financial statement audit.

OIG Evaluation of Leon Snead & Company's Audit Performance

We reviewed LSC's report and related documentation and made necessary inquiries of its representatives. Our review was not intended to enable the OIG to express, and we do not express an opinion on the FEC's financial statements; nor do we provide conclusions about the effectiveness of internal control or conclusions on FEC's compliance with laws and regulations. However, the OIG review disclosed no instances where LSC did not comply, in all material respects, with *Government Auditing Standards.*

We appreciate the courtesies and cooperation extended to LSC and the OIG staff during the audit. If you should have any questions concerning this report, please contact my office on (202) 694-1015.

Lynne A. McFarland
Inspector General

Attachment

cc: Judy Berning, Acting Chief Financial Officer
Alec Palmer, Staff Director/Chief Information Officer
Gregory Baker, Deputy General Counsel for Administration
Lisa Stevenson, Deputy General Counsel for Law

Federal Election Commission

Audit of Financial Statements

As of and for the Years Ended September 30, 2014 and 2013

Submitted By

Leon Snead & Company, P.C.
Certified Public Accountants & Management Consultants

TABLE OF CONTENTS

Page

LEON SNEAD
& COMPANY, P.C.

Certified Public Accountants
& Management Consultants

416 Hungerford Drive, Suite 400
Rockville, Maryland 20850
301-738-8190
Fax: 301-738-8210
leonsnead.companypc@erols.com

Independent Auditor's Report

THE COMMISSION, FEDERAL ELECTION COMMISSION
INSPECTOR GENERAL, FEDERAL ELECTION COMMISSION

We have audited the accompanying financial statements of Federal Election Commission (FEC), which comprise the balance sheet as of September 30, 2014 and 2013, and the related statements of net cost, changes in net position, budgetary resources, and custodial activity for the years then ended. The objective of our audit was to express an opinion on the fair presentation of those financial statements. In connection with our audit, we also considered the FEC's internal control over financial reporting, and tested the FEC's compliance with certain provisions of applicable laws, regulations, and certain provisions of contracts.

SUMMARY

As stated in our opinion on the financial statements, we found that the FEC's financial statements as of and for the years ended September 30, 2014 and 2013, are presented fairly, in all material respects, in conformity with accounting principles generally accepted in the United States of America.

Our consideration of internal control would not necessarily disclose all deficiencies in internal control over financial reporting that might be material weaknesses under standards issued by the American Institute of Certified Public Accountants. Our testing of internal control identified no material weakness in internal controls over financial reporting. However, we identified a significant deficiency related to the Information Technology (IT) security program established by the FEC. We also noted one other control issue that did not rise to the level of a reportable condition which is included in a separate letter, dated November 14, 2014, for management's consideration.

It should be noted that during this fiscal year, FEC has initiated actions to address many of the findings and recommendations in our 2013 audit report. For example, the agency has taken actions to close 9 of the 27 open audit recommendations, and has obtained software, hardware, and technical support services totaling in excess of $1.5 million, to date, to address findings and recommendations in the audit report.

Our tests of compliance with certain provisions of laws, regulations, and significant provisions of contracts, disclosed one instance of noncompliance that is required to be

reported under *Government Auditing Standards* and the OMB audit bulletin. This issue deals with noncompliance with The Homeland Security Presidential Directive 23 and National Security Presidential Directive 54, *Cyber Security and Monitoring,* establishing the Comprehensive National Cyber Security Initiative, and relating to Initiative No. 1, *Manage the Federal Enterprise Network as a Single Enterprise with a Trusted Internet Connection (TIC).*

The following sections discuss in more detail our opinion on the FEC's financial statements, our consideration of the FEC's internal control over financial reporting, our tests of the FEC's compliance with certain provisions of applicable laws and regulations, and management's and our responsibilities.

REPORT ON THE FINANCIAL STATEMENTS

We have audited the accompanying financial statements of FEC, which comprise the balance sheets as of September 30, 2014 and 2013, and the related statements of net cost, statements of changes in net position, statements of budgetary resources, and custodial activity for the years then ended, and the related notes to the financial statements.

Management's Responsibility for the Financial Statements

Management is responsible for the preparation and fair presentation of these financial statements in accordance with accounting principles generally accepted in the United States of America. Such responsibility includes the design, implementation, and maintenance of internal control relevant to the preparation and fair presentation of financial statements that are free from material misstatement, whether due to error or fraud.

Auditor's Responsibility

Our responsibility is to express an opinion on the financial statements based on our audit. We conducted our audit in accordance with auditing standards generally accepted in the United States of America; standards applicable to financial statement audits contained in *Government Auditing Standards (GAS)*, issued by the Comptroller General of the United States; and OMB Bulletin 14-02, *Audit Requirements for Federal Financial Statements* (the OMB audit bulletin). Those standards and the OMB audit bulletin require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free from material misstatement.

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the financial statements. The procedures selected depend on the auditor's professional judgment, including the assessment of the risks of material misstatement of the financial statements, whether due to fraud or error. In making those risk assessments in a Federal agency, the auditor considers internal control relevant to the entity's preparation and fair presentation of the financial statements in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of

expressing opinions on the effectiveness of the FEC's internal control or its compliance with laws, regulations, and significant provisions of contracts. An audit also includes evaluating the appropriateness of accounting policies used, and the reasonableness of significant accounting estimates made by management, as well as evaluating the overall presentation of the financial statements.

We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our audit opinion.

Opinion

In our opinion, the financial statements referred to above present fairly, in all material respects, the financial position of FEC as of September 30, 2014 and 2013, and the related net cost, changes in net position, budgetary resources, and custodial activity for the years then ended in accordance with accounting principles generally accepted in the United States of America.

OTHER MATTERS

Required Supplementary Information

Accounting principles generally accepted in the United States require that Management's Discussion and Analysis (MDA) be presented to supplement the basic financial statements. Such information, although not a part of the basic financial statements, is required by the Federal Accounting Standards Advisory Board (FASAB) who considers it to be an essential part of financial reporting for placing the basic financial statements in an appropriate operational, economic, or historical context. We have applied certain limited procedures to the required supplementary information in accordance with auditing standards generally accepted in the United States of America, which consisted of inquiries of management about the methods of preparing the information and comparing the information for consistency with management's responses to our inquiries, the basic financial statements, and other knowledge we obtained during our audit of the basic financial statements. We do not express an opinion or provide any assurance on the information because the limited procedures do not provide us with sufficient evidence to express an opinion or provide any assurance.

Other Information

Our audit was conducted for the purpose of forming an opinion on the basic financial statements taken as a whole. The performance measures and other accompanying information are presented for the purposes of additional analysis and are not required parts of the basic financial statements. Such information has not been subjected to the auditing procedures applied in the audit of the basic financial statements, and accordingly, we do not express an opinion or provide any assurance on it.

OTHER AUDITOR REPORTING REQUIREMENTS

Report on Internal Control

In planning and performing our audit of the financial statements of FEC, as of and for the years ended, September 30, 2014 and 2013, in accordance with auditing standards generally accepted in the United States of America, we considered the FEC's internal control over financial reporting (internal control) as a basis for designing audit procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the FEC's internal control. Accordingly, we do not express an opinion on the effectiveness of the FEC's internal control.

Our consideration of internal control was for the limited purpose described in the preceding paragraph and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies. Therefore, material weaknesses or significant deficiencies may exist that were not identified. However, given these limitations, during our audit, we did not identify any deficiencies in internal control that we consider to be a material weakness. As discussed below, we identified a deficiency in internal control that we consider to be a significant deficiency.

Because of inherent limitations in internal controls, including the possibility of management override of controls, misstatements, losses, or noncompliance may nevertheless occur and not be detected. A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. A material weakness is a deficiency or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Findings and Recommendations

FEC IT Security Program Does Not Yet Meet Applicable IT Security Best Practices *(Modified Repeat Findings)*

FEC has initiated corrective actions[1] on many of our prior year's audit recommendations; advised us that the agency has completed corrective actions on eight (8) others[2]; and has contracted for a review of IT security operations to identify gaps between FEC's current IT security controls and best practice controls, and the costs to meet identified security

[1] FEC officials provided us with documentation detailing the actions being taken and planned to address the audit recommendations in the 2013 financial statement audit.

[2] This information was not subjected to the auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on it at this time.

gaps. Although the agency is currently gathering this review information, it has not yet agreed to adopt applicable IT security best practices[3] which can improve the agency's IT security program. A decision on this key area will not be made until after the completion of the review contract, scheduled for May 2015. Governance has emphasized improving IT security within the agency, and FEC officials have implemented actions that reduce risks to its information and information systems. However, until corrective actions are fully implemented, including the adoption of applicable government-wide IT security best practices, the agency's information and information systems remain at risk.

As required by GAS, we conducted follow-up testing to determine whether FEC had implemented corrective actions to address the findings and recommendations in the FY 2013 FEC financial statement audit. The following paragraphs detail the actions taken by the agency to address the open findings and recommendations, and, as appropriate, our analysis of these actions.

a. <u>Information Technology Security Best Practices Need to be Implemented</u>

FEC financial statement audit reports issued since 2009 have recommended that the agency adopt federal government IT security best practices as other agencies have done that are also exempt from the Federal Information Security Management Act (FISMA) requirements. Our prior audits have also recommended that FEC officials make a risk-based analysis to support the agency's decision to not adopt minimum government-wide IT security requirements, and document these decisions. We reported in prior audits that the agency made decisions to reject government IT security requirements based upon whether the agency was exempt from the legislative requirement, rather than making a risk-based assessment to determine if the control would provide an effective reduction of risks to FEC's information and information systems. **(See Recommendation Nos. 1 & 2)**

On August 15, 2014, the FEC awarded a contract to identify and document gaps between best practices IT security controls and FEC's existing security controls, and to provide a "…cost analysis for implementing the recommended security controls. The scope of this project is extensive and will require the contractor to map the FEC's information systems, develop a high-level understanding of the FEC's strategic dependency on each system and the information it contains, develop an analysis of the impact that a loss of the Confidentiality, Integrity or Availability of the information contained in each system would have on the agency and formally document the organizational impact statement for each information system and the mission impact in the event of a loss of Confidentiality, Integrity or Availability of that information. This process will establish the initial baseline of security controls for each system necessary to fully understand the FEC's risks and

[3] IT security best practices are detailed in National Institute of Standards and Technology (NIST) Special Publication No. 53, Recommended Security Controls for Federal Information Systems and Organizations, and other related NIST publications. The (best practices) IT controls detailed in these documents provide generally accepted minimum control processes that provide a sufficient level of security to protect FEC's information and information systems.

needs as defined by FIPS 199, FIPS 200 and SP 800-53." At the completion of the contract, the contractor will prepare a report of recommendations of the costs for and resources needed to implement any or all of NIST. The agency advised us that this information, due in May 2015, will be used to determine whether the agency will adopt any or all applicable IT security best practices. Additionally, the FEC's FY 2015 draft budget includes approximately $500,000 to implement NIST IT controls, including but not limited to hiring staff and purchasing tools."

We believe that the actions taken by FEC's governance during FY 2014 reflect positive steps in addressing this long standing problem area. With the data provided by the contractor, the agency will have sufficient information to make risk-based decisions.

b. <u>Planning, Oversight and Monitoring of FEC's Corrective Action Plan (CAP)</u>

FEC has made progress in addressing problems reported in prior years' concerning the lack of effective corrective actions. Of the 27[4] prior year recommendations, 9 have been closed, and FEC has advised us that corrective actions are ongoing on the remaining recommendations. However, we believe that additional progress could have been made had the agency developed more comprehensive project plans that include: key tasks, assignments, timeframes, resource information, and other necessary information. **(See Recommendations Nos. 3, 4 and 17)**

<u>Oversight and Monitoring of CAP</u>

FEC had not timely implemented actions necessary to remediate weaknesses in IT controls, some of which we first reported in 2009, as required by OMB's Circular A-123, *Management's Responsibility for Internal Control*, Section II.E and Section V, or OMB's Circular A-50, *Audit Follow-up*. During our FY 2014 financial statement audit, we tested the actions taken by FEC to address the audit recommendations included in our 2013 audit report. Our FY 2014 audit found that for the first time since reporting on IT control weaknesses in our FY 2009 financial statement audit report, FEC has begun to take significant actions to address some of the more critical IT security deficiencies that impact the agency's information and information systems. As discussed later in this report, FEC governance over the past year has taken significant actions to improve the agency's IT infrastructure overall; the agency's IT security posture specifically; and has a plan to continue IT enhancements in future years.

However, until all corrective actions are fully implemented, including adoption of government-wide IT security best practices, the agency's systems remain at risk.

[4] The 2013 financial statement audit report included a recommendation to implement the CAP developed by the CISO to address the October 2012 *Threat Assessment Program* (Mandiant) Report. The open recommendations from the Mandiant report are included in the 27 open recommendations (see recommendation no. 3).

Planning for Corrective Actions

During our FY 2014 audit, we requested individual project plans relating to corrective actions on 16 of the recommendations in the 2013 financial statement audit report. We selected these 16 from the 27 recommendations in the report because the level of effort involved in implementing the recommendation would require a detailed project plan. For example, corrective actions for several areas were estimated to last a year or more, involved use of contractors on a large scale, many FEC offices, and complex, interrelated tasks. However, when we requested project plans for these tasks, we were advised by FEC officials that detailed plans were not required, and it was up to the project leader to ensure that the tasks are completed in an effective and timely manner. These officials further advised that the agency's "FY 2013 Financial Statement Audit Corrective Action Plan (CAP)" provides information on each specific project and its status.

We reviewed the CAP to determine if it met Project Management Body of Knowledge (PMBOK) guidelines[5]; or could be used in any meaningful manner to track the specific tasks for the project, the estimated and actual timeframes for initiation and completion of the actions, or other key project management requirements. Our review of this document determined that it could not be used in any meaningful manner to meet either of the above criteria.

In addition, we believe that FEC Directive 50, *Audit Follow-up*, requires agency personnel to develop more comprehensive corrective action planning documents. For example, Directive 50 requires personnel to "… (1) Develop a written corrective action plan, including specific steps and/or tasks to be taken to implement the corrective action plan and a projected time frame for completion of each step or task." Directive 50 also notes that "…reports shall include the status of all unresolved audit reports, the outstanding steps or tasks required to be completed in order to resolve the recommendations raised in the audit report, and a timetable for resolution of those steps or tasks…"

The FEC CAP for the 2013 audit meets few, if any, of the requirements of Directive 50, and would not be a meaningful substitute for proper project planning. Due to a lack of proper planning, FEC has struggled in prior years to implement corrective actions that address the vulnerabilities to FEC's information and information systems.

c. Assessment and Accreditation of the General Support System (GSS)

The FEC has not completed a full assessment and accreditation of its GSS, or updated its policies relating to assessment and accreditation. In our 2013 financial statement audit, we reported that: "FEC needs to perform an assessment of its

[5] A Guide to the Project Management Body of Knowledge (PMBOK Guide), issued by the Project Management Institute, and recognized by the American National Standards Institute (ANSI), and the Institute of Electrical and Electronics Engineers, establishes standards and guidelines for effective project management (best practices).

general support system to identify vulnerabilities that could allow further network intrusions and data breaches. In addition, FEC has not followed FEC (Office of the Chief Information Officer (OCIO) policy 58-2.4, *Certification and Accreditation Policy*, which establishes controls over the process of obtaining independent assurance that FEC major applications and general support system (GSS) are capable of enforcing the security policies that govern their operations." During our 2014 audit, we discussed this problem area with FEC officials. FEC officials advised us that a risk assessment was completed by Department of Homeland Security (DHS), and that this risk assessment addressed the audit recommendation. **(See Recommendation Nos. 13 & 14)**

Our review of the report showed that DHS used the National Institute of Standards and Technology (NIST) controls and conducted a limited scope review that included web scanning, penetration testing, and phishing tests of selected control areas. We noted eight applicable control areas were not tested. As all controls applicable to the FEC's business processes were not tested, this limited scope review was not sufficient, by itself, to meet best practice testing required of a system's security plan[6] in order to accredit the system.

d. <u>Access Controls and Recertification of Users' Access Authorities</u>

In prior audits, we reported weaknesses in overall access controls within the agency, including the need for a periodic review of users' access authorities[7]. These control weakness were first reported in our 2009 financial statement audit report, and FEC corrective actions to address this problem area were not effective and/or fully implemented; therefore, access control weaknesses continue to be an issue in FY 2014. **(See Recommendation Nos. 5, 6, 9, 10 & 11)**

Our FY 2014 financial statement audit testing identified that FEC has begun to implement corrective actions to address these problem areas. For example, FEC officials advised us that the agency has appointed the Chief Information Security Officer (CISO) as the project manager, and has establish procedures for performing periodic reviews of users' access authorities. FEC officials noted that they have obtained additional resources to implement this IT control, additional access controls will be implemented by November 2014, and estimated that by mid-March 2015, processes will be in place to review users' access authorities annually.

[6] FEC had not performed an assessment of its key medium risk GSS since December 2008.

[7] Periodic reviews of users access authorities is an IT security control required by best practices, and FEC's own policies. IT policy 58-2.2, Account Management Policy, states "All user account access rights and privileges will be periodically reviewed and validated in accordance with General Support System...system security plans..." The security plan for the General Support System, dated 2009, contains a control requirement that the users' accounts will be reviewed every six months.

e. Configuration Management and Vulnerability Scanning Programs

FEC needs to continue to strengthen its configuration security controls by completing its project to implement U.S. Government Configuration Baseline (USGCB)[8] security configurations. In addition, FEC's vulnerability scanning program (which tests that established configuration requirements have been implemented) did not meet best practices; and system vulnerabilities identified from the scanning process were not timely mitigated. **(See Recommendation Nos. 7, 8 & 12)**

FEC officials advised us that the FEC has made progress on the implementation of USGCB requirements. FEC has divided this project into five groups, has completed testing for three of the five groups, and is working toward having the control fully deployed by the end of December 2014. Concerning security patches and vulnerability scanning, FEC officials advised that actions are being taken in these areas also. For example, FEC has established controls that require servers to be scanned and patched monthly. Concerning laptops and desktop computers, FEC has just implemented controls to patch these types of devices, and perform scanning on a monthly basis.

f. Continuity of Operations Plan (COOP)

FEC has not yet fully and effectively tested and exercised the Continuity of Operations Plan (COOP) – a critical element in the development of a comprehensive and effective plan. As discussed in Federal Continuity Directive (FCD) No. 1[9], until the COOP plan is tested and exercised, any deficiencies in the plan cannot be determined, and the agency remains at risk of not being able to carry out the mission of the agency in the event of a disruption to normal business operations. **(See Recommendation Nos. 15 & 16)**

[8] OMB M-08-22: In March 2007, OMB Memorandum M-07-11 announced the "Implementation of Commonly Accepted Security Configurations for Windows Operating Systems," directing agencies … to adopt the Federal Desktop Core Configuration (FDCC) security configurations developed by the National Institute of Standards and Technology (NIST), the Department of Defense and the Department of Homeland Security. The USGCB is the security configuration and policy developed for use on Federal government Windows 7 and Internet Explorer 8 and as stated by the CIO Council, 'the USGCB initiative falls within FDCC and comprises the configuration settings component of FDCC.'

[9] Federal Continuity Directive No.1, Federal Executive Branch National Continuity Program, Appendix K, Test, Training and Exercise, require that COOP documents must be validated through tests, training, and exercises (TT&E), and that all agencies must plan, conduct, and document periodic TT&Es to prepare for all-hazards continuity emergencies and disasters, identify deficiencies, and demonstrate the viability of their continuity plans and programs. Deficiencies, actions to correct them, and a timeline for remedy must be documented in an organization's CAP (corrective action plan). FEC Policy No. 58.2.9 provides that plans should not be considered valid until tested for practicality, executability, errors and/or omissions. The initial validation test should consist of a simulation or tactical test. Once validated, plans should be tested annually, or when substantive changes occur to the system, to the system environment, or to the plan itself. Test results should be maintained in a journal format and retained for analysis. Validated change recommendations resulting from testing activities should be incorporated into plans immediately.

FEC officials have advised us that funds have been approved to replace obsolete equipment; the agency is updating the COOP, and intends to create a milestone plan to complete this project.

FEC officials provided information showing the actions FEC is taking to strengthen its IT security program. A summary of the information provided to us is discussed below.

"The FEC understands the importance of IT security and is committed to the timely implementation of the FY 2013 Financial Statement Audit Corrective Action Plan (CAP). Over the past year, the FEC has taken significant actions to improve the agency's IT infrastructure generally and our IT security posture specifically and the agency has a robust plan and leadership support to continue IT enhancements in future years. Many of the Commission's future decisions with respect to IT security enhancements will be informed by the ongoing NIST study, with results to be reported in or about May 2015…."

FEC officials also advised that "While the FEC faces budgetary challenges across the full range of its activities and divisions, a unanimous Commission has placed special emphasis on the audit corrective process over the past year." These officials further advised that the agency increased the IT budget by"… $640,000 over the planned budget for FY 2014. The additional $640,000 was specifically targeted to addressing issues raised in the FY 2013 Financial Statement Audit…With the increased funding corrective actions are underway for most of the areas reported in the FY 2013 Financial Statement Audit. Although work remains to be completed, the agency has seen a number of IT security successes over the past year…"

FEC officials advised that "… the FEC has moved forward to aggressively address IT security vulnerabilities and enhance OCIO's ability to detect and deter cyber threats. During FY 2014, OCIO successfully completed a number of IT security projects that have already substantially improved the agency's IT security posture…" Some of the projects identified by FEC officials are as follows:

- In January 2014, OCIO completed a risk vulnerability assessment that identified those network assets at highest risk and assessed potential vulnerabilities and impacts. Results from this assessment have already helped to inform decisions regarding how best to protect the FEC's networks and to establish audit readiness.
- OCIO has implemented (a) tool…to identify missing patches and areas of vulnerability in managed devices and mitigate those security risks.
- OCIO has launched (a tool)…to detect and stop web-based and email attacks that exploit emerging, "zero-day" vulnerabilities.
- OCIO has improved the security of its web servers….
- Security for the electronic filing system has been enhanced through implementation of firewall security software.
- OCIO initiated a project to…provide unified security monitoring and analytics….

- In September 2014, the FEC acquired an additional tool…to help OCIO identify, rank and remove vulnerabilities early in the software development process and help OCIO find and fix security issues with software, code and applications. This tool will be fully implemented during FY 2015.
- OCIO has additionally taken concrete steps during FY 2014 to meet crucial milestones for projects to be completed in future years. For example, in October 2013, OCIO began work on an ongoing effort, in partnership with the Department of Homeland Security (DHS), to employ continuous vulnerability scanning and cyber hygiene monitoring. In February 2014, the FEC put in place an agreement with DHS and… (a vendor) to deploy Intrusion Prevention System capabilities during FY 2015.

We believe the actions, as discussed above, taken by governance during FY 2014 to address the longstanding problems discussed in our 2013 audit report are significant steps that should strengthen FEC's IT security program and reduce risk to the agency's information and information systems. These actions enabled us to close 9 of the 27 recommendations in the 2013 audit. In addition, we have been advised that corrective actions have recently been completed to address additional open audit recommendations.

Listed below are open *(repeat)* recommendations from our FY 2013 financial statement audit report, and a recommendation to address issues relating to project planning that was first addressed in FY 2014.

Recommendations

1. Formally adopt as a model for FEC, the NIST IT security controls established in FIPS 199, FIPS 200, SP 800-53, and other applicable guidance that provides best practice IT security control requirements. *(Repeat)*

   Agency's Response

   The OCIO concurs with this recommendation. The OCIO awarded a contract in August 2014 to obtain a system inventory, GAP analysis, and provide study results concerning the feasibility in cost of implementing NIST Guidelines. Phase I of work started in September 2014. This phase is for Systems Inventory portion and expected to conclude by the end of November 2014. Phase II will then begin by December 2014, which will be the GAP/Analysis portion of this contract. It is expected to conclude approximately in April 2015. At the end of Phase II the contractor will prepare a report of recommendations of cost and resources needed to implement any or all of NIST.

   Auditor's Comments

   OCIO officials have agreed to implement this recommendation; however, until FEC adopts government-wide IT security best practices, the agency's information and information systems remain at risk.

2. Revise FEC policies and procedures to require a documented, fact-based, risk assessment prior to declining adoption of any government-wide IT security best practice, or IT security requirement. Require the Chief Information Officer (CIO) to approve, and accept the risk of any deviation from government-wide IT security best practices that are applicable to the FEC business operations. Retain documentation of these decisions. *(Repeat)*

   Agency's Response

   The OCIO concurs with this recommendation. The policies and procedures will be updated upon completion of the study from recommendation no. 1 and the Commission's approval.

   Auditor's Comments

   Since OCIO officials have agreed to implement this recommendation, we have no additional comments.

3. Complete the implementation of the open contractor's recommendations contained in the October 2012 Threat Assessment Program report. Provide sufficient budgetary and personnel resources to this project to ensure that actions are properly accomplished. *(Modified Repeat)*

   Agency's Response

   The OCIO concurs with this recommendation. The OCIO has implemented all the core recommendations from the contractors report. Further, OCIO has implemented additional countermeasures to help the Agency respond to malicious attacks, such as FireEye, IPSS and Tenable Continuous View.

   Auditor's Comments

   Since OCIO officials have agreed to implement this recommendation, we have no additional comments.

4. Revise all pertinent FEC policies and procedures to ensure that they address proper prevention and detection controls, and provide a current and authoritative control structure for addressing Advance Persistent Threat (APT), and other types of intrusions. *(Modified Repeat)*

   Agency's Response

   The OCIO concurs with this recommendation. The agency expects to have documented standard operating procedures (SOPs) in place by November 2014. Once this action is completed the agency will consider this item closed.

   Auditor's Comments

   Since OCIO officials have agreed to implement this recommendation, we have no additional comments.

5. Complete the project relating to review of user access authorities, and ensure necessary budgetary and personnel resources are provided to complete this project. *(Modified Repeat)*

Agency's Response

The OCIO concurs with this recommendation and plans to implement user access authorities and reviews by mid February 2015.

Auditor's Comments

Since OCIO officials have agreed to implement this recommendation, we have no additional comments.

6. Reissue FEC Policy 58-2.2 to require annual recertification of users' access authorities by supervisory personnel who would have knowledge of the users' requirements for accessing FEC information and information systems. Ensure that the policy contains sufficient operational details to enable an effective review and update process. *(Repeat)*

Agency Response

The OCIO concurs with this recommendation and is the same as recommendation no. 5.

Auditor's Comments

Since OCIO officials have agreed to implement this recommendation, we have no additional comments.

7. Revise FEC policies and operating procedures to require the minimum best practices controls contained in the United States Government Configuration Baseline (USGCB). *(Modified Repeat)*

Agency's Response

The OCIO concurs with this recommendation and is currently working to implement USGCB by December 2014.

Auditor's Comments

Since OCIO officials have agreed to implement this recommendation, we have no additional comments.

8. Implement USGCB baseline configuration standards for all workstations and require documentation by the CIO to approve and accept the risk of any deviation. *(Modified Repeat)*

Agency's Response

The OCIO concurs with this recommendation and is the same as response no. 7.

Auditor's Comments

Since OCIO officials have agreed to implement this recommendation, we have no additional comments.

9. Undertake a comprehensive review of user accounts that have been granted non-expiring passwords. Require detailed information from account owners on the need for non-expiring accounts, including the development of other alternatives, before reauthorizing the accounts' access. Develop FEC policies and operating procedures to implement this recommendation. *(Repeat)*

Agency's Response

The OCIO concurs with this recommendation and considers it closed.

Auditor's Comments

OCIO officials have agreed to implement this recommendation, and advised that they believe the recommendation is closed.[10]

10. Whenever possible, require accounts with non-expiring passwords to be changed at least annually. Establish substantially more robust password requirements for accounts granted non-expiring passwords. Develop FEC policies and operating procedures to implement this recommendation. *(Repeat)*

Agency's Response

The OCIO concurs with this recommendation and considers it closed.

Auditor's Comments

OCIO officials have agreed to implement this recommendation, and advised that they believe the recommendation is closed.[11]

11. Immediately terminate those accounts with non-expiring passwords that have not accessed their accounts within the last 12 months. Develop FEC policies and operating procedures to implement this recommendation to include a data retention policy for historical data. *(Repeat)*

Agency's Response

The OCIO concurs with this recommendation and considers it closed.

[10] An independent evaluation of the actions taken by the agency has not been made as the corrective actions were not completed in the audit timeframe to be reviewed for the FY 2014 audit. Therefore, we offer no comments on the recommendation's closure status.

[11] See footnote 10.

Auditor's Comments

OCIO officials have agreed to implement this recommendation, and advised that they believe the recommendation is closed.[12]

12. Strengthen controls to ensure that vulnerabilities/weaknesses identified through the vulnerability scanning tests are completed within 60 days of identification, or document an analysis and acceptance of risks for longer term remediation. *(Repeat)*

Agency's Response

The OCIO concurs with this recommendation and considers it closed.

Auditor's Comments

OCIO officials have agreed to implement this recommendation, and advised that they believe the recommendation is closed.[13]

13. Perform within this fiscal year a new assessment and accreditation of the GSS using NIST SP 800-53 as the review criteria. *(Repeat)*

Agency's Response

The OCIO concurs with this recommendation and is the same as response no. 1.

Auditor's Comments

Since OCIO officials have agreed to implement this recommendation, we have no additional comments. (Also see our comments for recommendation no. 1)

14. Strengthen FEC Policy 58-2.4 so that it provides additional guidance on what decision points determine when a new assessment and accreditation is required; and the specific documentation requirements that need to be maintained in order for the agency to track changes so it can make informed decisions on when major changes drive the need for a new assessment and/or updated accreditation. *(Repeat)*

Agency's Response

The OCIO concurs with this recommendation and is the same as response no. 1.

Auditor's Comments

Since OCIO officials have agreed to implement this recommendation, we have no additional comments. (Also see our comments for recommendation no. 1)

[12] See footnote 10.
[13] See footnote 10.

15. Ensure that sufficient resources are assigned to the task of testing the COOP, a critical IT control process, in order to reduce risk to the FEC, and complete all required tests in a timely manner. Ensure that appropriate documentation is retained as required by FCD No. 1 to support that FEC has met all applicable federal requirements. *(Repeat)*

Agency's Response

The OCIO concurs with this recommendation and plans to move forward to implement this in the second quarter of 2015.

Auditor's Comments

Since OCIO officials have agreed to implement this recommendation, we have no additional comments.

16. Develop a detailed Plan of Action and Milestone (POA&M) to ensure that required COOP testing and exercises are completed as soon as possible. *(Repeat)*

Agency's Response

The OCIO concurs with this recommendation and plans to move forward to implement in FY 2015.

Auditor's Comments

Since OCIO officials have agreed to implement this recommendation, we have no additional comments.

17. Issue a FEC policy that requires project managers to prepare project plans that address FEC Directive 50 requirements for projects that are implemented to address audit recommendations. Require that the project plan includes information, such as: identification of key tasks and/or steps; personnel responsible for completing the task and/or step; the timeframe for beginning and completing the task and/or step; resources required; and that documentation be maintained, as part of the project plan, to support the accomplishment of key plan tasks, issues that impacted the project, and the completion of the overall project.

Agency's Response

The OCIO concurs with this recommendation in part. The agency concurs that the current financial statement CAP needs to be improved to provide more information to enable the audit follow-up officials and OIG to more effectively monitor the actions that are taking place. Management agrees to enhance the current CAP to provide additional information on the specific tasks and actions being taken to address findings and recommendations. Management will implement alternative corrective actions which are more efficient and will provide the information needed to address the intent of this recommendation.

Auditor's Comments

The agency concurs, in part, with this recommendation, and agrees that the current CAP needs to be improved. Until FEC completes its proposed corrective actions in this area, we are unable to determine whether these alternative actions will address the audit recommendation.

We noted another control deficiency over financial reporting that we do not consider a significant deficiency, but still needs to be addressed by management. We have reported this matter to FEC's management, and those charged with governance in a separate letter dated November 14, 2014.

A summary of the status of prior year recommendations is included as Attachment 1.

REPORT ON COMPLIANCE

As part of obtaining reasonable assurance about whether the agency's financial statements are free of material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, and significant provisions of contracts, noncompliance with which could have a direct and material effect on the determination of financial statement amounts, and certain other laws and regulations. We limited our tests of compliance to these provisions and we did not test compliance with all laws and regulations applicable to the FEC. Providing an opinion on compliance with certain provisions of laws, regulations, and significant contract provisions was not an objective of our audit and, accordingly, we do not express such an opinion.

In connection with our audit, we noted one instance described below of noncompliance that is required to be reported according to *Government Auditing Standards* and the OMB audit bulletin guidelines. No other matters came to our attention that caused us to believe that FEC failed to comply with applicable laws, regulations, or significant provisions of laws, regulations, and contracts that have a material effect on the financial statements insofar as they relate to accounting matters. Our audit was not directed primarily toward obtaining knowledge of such noncompliance. Accordingly, had we performed additional procedures, other matters may have come to our attention regarding the FEC's noncompliance with applicable laws, regulations, or significant provisions of laws, regulations, and contracts insofar as they relate to accounting matters.

Noncompliance with Comprehensive National Cyber Security Initiative

We first reported that the FEC was noncompliant with The Homeland Security Presidential Directive 23, and National Security Presidential Directive 54, *Cyber Security and Monitoring* in our FY 2012 audit report. These directives establish the Comprehensive National Cyber Security Initiative, and relate to Initiative No. 1, *Manage the Federal Enterprise Network as a Single Enterprise with a Trusted Internet Connection (TIC).*

TIC was introduced in OMB Memorandum M-08-05, *Implementation of Trusted Internet Connections*, dated November 20, 2007. The initiative was described in the memorandum as an effort to develop "a common [network] solution for the federal government" that would reduce the number of external Internet connections for the entire government. The memorandum stated that "each agency will be required to develop a comprehensive POA&M (Plan of Action and Milestones)" to implement TIC, but it neither defined "agency" nor referred to any legal authority supporting the initiative.

FEC's Office of General Counsel (OGC) analyzed this document and initially determined that the FEC was exempt from implementing TIC. However, at our request, OGC reassessed this determination, and in an August 2012 memorandum to the Staff Director, the OGC stated that "…we conclude that FEC must comply with all requirements of…TIC." Based upon this OGC opinion, FEC officials agreed in 2012 to implement TIC.

Our 2014 audit tests found that limited actions have been taken by the agency to address this Presidential directive. FEC officials advised us that the "OCIO has completed preparatory work to implement MTIPS—Trusted Internet Connection (TIC). However, the initial cost of implementing a TIC at the FEC is estimated at $555,000, which does not include substantial recurring costs necessary to maintain the system. The agency must consider whether to fund the TIC project during FY 2015 or other mission-critical projects. Throughout its efforts to improve the FEC's IT security posture and to implement the corrective action plan, the agency has remained mindful of the limits to its financial and staff resources and the need to ensure the most impactful results for the resources expended. By working with DHS on IT security projects, the FEC has saved approximately $900,000—freeing critical resources for other IT security initiatives. As the FEC moves forward to implement additional projects necessary to address audit recommendations, the Commission has indicated it will continue to proceed thoughtfully in order to ensure the best overall use of the agency's resources and the greatest long-term improvements to IT security systems."

We continue to believe that the FEC is in non-compliance with laws and regulations that have mandated since 2007 that agencies strengthen and consolidate internet connections, and implement Homeland Security Presidential Directive 23, and National Security Presidential Directive 54, *Cyber Security and Monitoring*. These directives establish the Comprehensive National Cyber Security Initiative, and relate to "Manage the Federal Enterprise Network as a Single Enterprise with a Trusted Internet Connection (TIC)".

Recommendation

18. Develop a time-phased corrective action plan to address the prompt implementation of Homeland Security Presidential Directive 23, and National Security Presidential Directive 54, Cyber Security and Monitoring. *(Repeat)*

Agency's Response

The OCIO concurs with this recommendation. However, we are currently under a Continuing Resolution for FY 2015 and do not have funding available to cover costs associated with this recommendation.

Auditor's Comments

OCIO officials have agreed this recommendation needs to be implemented, but that funding is unavailable to cover the costs. We continue to believe that the FEC should develop a plan to implement this long-standing presidential and DHS directive to adequately plan for the project's implementation.

Restricted Use Relating to Reports on Internal Control and Compliance

The purpose of the communication included in the sections identified as "Report on Internal Control" and "Report on Compliance" is solely to describe the scope of our testing of internal control over financial reporting and compliance, and to describe any material weaknesses, significant deficiencies, or instances of noncompliance we noted as a result of that testing. Our objective was not to provide an opinion on the design or effectiveness of the FEC's internal control over financial reporting or its compliance with laws, regulations, or provisions of contracts. The two sections of the report referred to above are integral parts of an audit performed in accordance with *Government Auditing Standards* in considering the FEC's internal control over financial reporting and compliance. Accordingly, those sections of the report are not suitable for any other purpose.

AGENCY'S RESPONSE

The Acting Chief Financial Officer (ACFO) responded to the draft report in an email dated November 12, 2014, in which the agency responses to each recommendation were provided, along with an overall agency comments section. We have included FEC's response to each recommendation, and our comments after each numbered recommendation, summarized its overall comments in this section of the report.

The ACFO commented that "while the FEC concurs with each of the IT findings identified in the audit report, we do not agree that these issues result in a significant deficiency for financial statement purposes. We noted the auditors IT findings are almost solely related to the FEC's general support system (GSS) rather than the financial systems, which are outsourced. The likelihood of a material misstatement occurring due to weaknesses in the FEC GSS environment is extremely low. The current levels of IT controls do not impact the fair presentation of the agency's financial statements such that it would rise to the level of a significant deficiency in the scope of the financial statement audit."

AUDITOR'S COMMENTS

FEC officials concurred with 17 of the 18 recommendations, and concurred in part with the remaining recommendation in this report. However, FEC officials did not agree that these weaknesses should be reported as a significant deficiency in the financial statement audit report.

We disagree with FEC's position that the reported findings are not a significant deficiency. As noted in management's response, the OCFO has implemented many compensating controls to reduce the risk of misstatements in the financial statements; however, these compensating controls cannot mitigate the increased risk from all the IT control weaknesses identified. For instance, OCFO's compensating controls cannot mitigate the risk of the agency not having a fully implemented and tested Continuity of Operations Plan (COOP) to recover the Enterprise Content Management system (which resides on the GSS) that contains the OCFO's financial information. We conducted our audit of the FEC financial statements in accordance with professional standards as specified within this report. Our reporting of these IT control weaknesses which resulted in a significant deficiency in internal control meets the reporting standards discussed in these documents.

The FEC's November 12, 2014, response to the audit is included in its entirety as Attachment 2. The FEC's response was not subjected to the auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on it.

Leon Snead & Company, P.C.
November 14, 2014

Status of Prior Year Recommendations

Rec. No.	Recommendation	Recommendation Status
1.	Formally adopt as a model for FEC, the NIST IT security controls established in FIPS 199, FIPS 200, SP 800-53, and other applicable guidance that provides best practice IT security control requirements.	Open
2.	Revise FEC policies to require that FEC contractors adhere to the FAR requirements which adopt FISMA and NIST IT security controls that contractors must follow when providing services to the federal government.	Closed
3.	Revise FEC policies and procedures to require a documented, fact-based, risk assessment prior to declining adoption of any government-wide IT security best practice, or IT security requirement, including those that FEC may be legally exempt. Require the Chief Information Officer (CIO) to approve, and accept the risk of any deviation from government-wide IT security best practices that are applicable to the FEC business operations. Retain documentation of these decisions.	Open
4.	Using the initial Corrective Action Plan (CAP) developed by the Chief Information Security Officer as a base, implement each of the contractor's recommendations in the October 2012 *Threat Assessment Program* report, and complete all remedial actions (i.e. changing of all user passwords) within the next 60 days, and all other tasks by February 2014. Provide sufficient budgetary and personnel resources to this project to ensure that actions are properly accomplished.	Open
5.	Provide biweekly updates to the CIO on the status of the implementation of the October 2012 *Threat Assessment Program* report recommendations to ensure that it continues on track, and issues that arise are addressed as soon as possible.	Closed
6.	Provide semiannual corrective action plan (CAP) updates to the Commission on the status of the implementation of the October 2012 Threat Assessment Program report recommendations in accordance with Commission Directive 50.	Closed
7.	Revise all pertinent FEC policies and procedures to ensure that they address proper prevention and detection controls, and provide a current and authoritative control structure for addressing APT, and other types of intrusions. Ensure that this review is completed, and policies and procedures are issued by March 2014.	Open
8.	Assure that the annual performance plans of all appropriate audit follow-up officials reflect their responsibility to monitor and ensure the timely implementation of audit recommendations, as required by OMB Circular A-50.	Closed
9.	Require the audit follow-up official to develop a tracking process that would include monthly reports to the CIO, and highlight key tasks, progress, and missed target dates, when applicable.	Closed
10.	Establish a project (relating to review of user access authorities) with the project manager reporting to the CIO to help ensure that this long-delayed project will be implemented within the next three months. Require the project director to provide biweekly updates to the CIO.	Open

	Provide necessary budgetary and personnel resources to ensure that this project is completed timely.	
11.	Reissue FEC Policy 58-2.2 to require annual recertification of users' access authorities by supervisory personnel who would have knowledge of the users' requirements for accessing FEC information and information systems. Ensure that the policy contains sufficient operational details to enable an effective review and update process.	Open
12.	Revise FEC policies and operating procedures to require the minimum best practices controls contained in the United States Government Configuration Baseline (USGCB) for those systems that require user identification and passwords.	Open
13.	Undertake a comprehensive review of user accounts that have been granted nonexpiring passwords. Require detailed information from account owners on the need for non-expiring accounts, including the development of other alternatives, before reauthorizing the accounts' access. Develop FEC policies and operating procedures to implement this recommendation.	Open
14.	Whenever possible, require accounts with non-expiring passwords to be changed at least annually. Establish substantially more robust password requirements for accounts granted non-expiring passwords. Develop FEC policies and operating procedures to implement this recommendation.	Open
15.	Immediately terminate those accounts with non-expiring passwords that have not accessed their accounts within the last 12 months. Develop FEC policies and operating procedures to implement this recommendation to include a data retention policy for historical data.	Open
16.	Strengthen controls over the establishment of initial and replacement (default) passwords, to include requiring that random passwords be used, and the default passwords used be changed monthly. Develop FEC policies and operating procedures to implement this recommendation.	Closed
17.	Establish written procedures and develop a policy for FEC contractor computer orientation that requires contractors to create their own unique login passphrase. Also, ensure that all current contractors have created their own unique login passphrase.	Closed
18.	Include all components of the general support system (GSS), including employees' workstations, and other FEC devices and applications into the organization's vulnerability/security scanning process and ensure that they are assessed at least semi-annually.	Closed
19.	Strengthen controls to ensure that vulnerabilities/weaknesses identified through the vulnerability scanning tests are completed within 60 days of identification, or document an analysis and acceptance of risks for longer term remediation.	Open
20.	Implement baseline configuration standards for all workstations and require documentation by the CIO to approve and accept the risk of any deviation.	Open
21.	Implement automated logging of all configuration changes and review logs regularly to ensure that all system changes, including changes to workstations, are processed through the change management framework.	Closed
22.	Fully implement USGCB standards and perform scanning of Internet Explorer configuration settings.	Open
23.	Perform within this fiscal year a new assessment and accreditation of the GSS using NIST SP 800-53 as the review criteria.	Open

24.	Strengthen FEC Policy 58-2.4 so that it provides additional guidance on what decision points determine when a new assessment and accreditation is required; and the specific documentation requirements that need to be maintained in order for the agency to track changes so it can make informed decisions on when major changes drive the need for a new assessment and/or updated accreditation.	Open
25.	Ensure that sufficient resources are assigned to the task of testing the COOP, a critical IT control process, in order to reduce risk to the FEC, and complete all required tests in a timely manner. Ensure that appropriate documentation is retained as required by FCD No. 1 to support that FEC has met all applicable federal TT&E requirements.	Open
26.	Develop a detailed POA&M to ensure that required COOP testing and exercises are completed as soon as possible.	Open
27.	Develop a time-phased corrective action plan to address the prompt implementation of the TIC by FEC.	Open

Agency Response to Report

While the FEC concurs with each of the IT findings identified in the audit report, we do not agree that these issues result in a significant deficiency for financial statement purposes. We noted the auditors IT findings are almost solely related to the FEC's general support system (GSS) rather than the financial systems, which are outsourced. The likelihood of a material misstatement occurring due to weaknesses in the FEC GSS environment is extremely low.

The current levels of IT controls do not impact the fair presentation of the agency's financial statements such that it would rise to the level of a significant deficiency in the scope of the financial statement audit. A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis.[14] Since 2004, the agency has substantially reduced financial risks over financial reporting by:

(1) Changing the information technology environment in FY 2008 by outsourcing the financial management system and financial management services;
(2) Implementing a number of manual reconciliations and other compensating controls over financial management areas and transactions significant to the financial statements; and
(3) Eliminating financial weaknesses identified in prior audit reports.

Since 2004, the agency has drastically changed their IT environment from maintaining an internal financial management system (PeopleSoft) and producing financial statements in-house to leveraging shared service providers to provide the agency's financial management system, which is used to maintain the agency's general ledger and produce the financial statements. FEC personnel do not have the ability to enter financial data directly into the financial management system.

The agency has substantially reduced financial risks over financial reporting and reduced the financial risks imposed by existing weaknesses in the FEC's IT environment by establishing and maintaining internal controls that provide reasonable assurance that the agency provides reliable financial reporting through compensating controls such as manual reconciliations. These reconciliations act to ensure the completeness, accuracy and validly of recorded transactions within the financial management system and the payroll system, which significantly reduce financial risks over financial reporting. Competed financial transactions must be manually reviewed by FEC personnel other than the preparer prior to submission to the external service provider for processing. The external service provider may only process actions in accordance with the listing of authorized signatures that have approving authority provided by the Acting CFO and verified by manual review by the external service provider. If an unauthorized

[14] AU-C 265, *Communicating Internal Control Related Matters Identified in an Audit*

transaction were to occur due to a weakness in the FEC IT environment the agency's manual reconciliations would catch the error.
The agency receives and now manually reviews reports from the external service providers on the Statements on Standards for Attestation Engagements (SSAEs) No. 16 *Reporting on Controls at a Service Organization* to identify existing controls and identify areas where the OCFO may need to implement a compensating control as applicable to FEC operational controls.

The agency has implemented improved quality review procedures as it relates to financial reporting to prevent and detect financial misstatements in a timely manner in the normal course of business. Therefore, in management's view the IT control risks identified do not rise to the level of a significant deficiency in the scope of the financial statement audit, as financial risks are effectively mitigated with compensating controls. The audit opinions issued in FY 2012, FY 2013, and FY 2014 recognize that the agency has implemented and maintained an effective financial reporting control environment, as the agency has not reported any significant deficiencies or material weakness over financial reporting over the past three years and received unqualified and unmodified opinions since 2004.

Federal Election Commission
Office of Inspector General

Fraud Hotline
202-694-1015

or toll free at 1-800-424-9530 (press 0; then dial 1015)
Fax us at 202-501-8134 or e-mail us at oig@fec.gov
Visit or write to us at 999 E Street, N.W., Suite 940, Washington DC 20463

Individuals including FEC and FEC contractor employees are encouraged to alert the OIG to fraud, waste, abuse, and mismanagement of agency programs and operations. Individuals who contact the OIG can remain anonymous. However, persons who report allegations are encouraged to provide their contact information in the event additional questions arise as the OIG evaluates the allegations. Allegations with limited details or merit may be held in abeyance until further specific details are reported or obtained. Pursuant to the Inspector General Act of 1978, as amended, the Inspector General will not disclose the identity of an individual who provides information without the consent of that individual, unless the Inspector General determines that such disclosure is unavoidable during the course of an investigation. To learn more about the OIG, visit our Website at: http://www.fec.gov/fecig/fecig.shtml

Together we can make a difference.